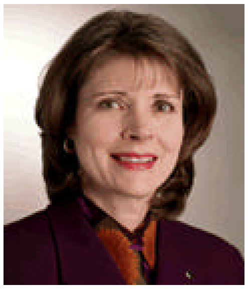
Homeland Security Technologies: Creating an Asymmetric Advantage

Dr. Ruth David
President and CEO — ANSER (Analytic Services Inc.)
April 2002



Dr. Ruth A. David is President and Chief Executive Officer of ANSER, an independent, nonprofit public service research institute that provides research and analysis support on national and transnational issues. In November 1999, Dr. David initiated ANSER's Homeland Defense Strategic Thrust to address the growing national concern of multi-dimensional, asymmetric threats from rogue nations, sub-state terrorist groups, and domestic terrorists. In May 2001, the ANSER Institute of Homeland Security was established to enhance public awareness and education and contribute to the dialog on a national, state, and local level.

Dr. David is a Member of the Corporation for the Charles Stark Draper Laboratory, Inc., and serves on the National Security Agency Advisory Board, the National Research Council Naval Studies Board, and the Senate Select Committee on Intelligence Technical Advisory Group. She previously served on the Defense Science Board, the Department of Energy Nonproliferation and National Security Advisory Committee and the Securities and Exchange Commission Technical Advisory Group. As the former Deputy Director for Science and Technology at the Central Intelligence Agency, Dr. David was responsible for research, development, and deployment of technologies in support of all phases of the intelligence process. She also represented the CIA on numerous national committees and advisory bodies, including the National Science and Technology Council and the Committee on National Security. Prior to joining the CIA, Dr. David spent 20 years in technical staff and leadership positions at Sandia National Laboratories in Albuquerque, New Mexico. She earned a Bachelor of Science in Electrical Engineering from Wichita State University, and her Masters and Doctoral degrees, also in Electrical Engineering, from Stanford University. She is a former adjunct professor at the University of New Mexico and coauthor of three technical reference books as well as numerous published papers.

The terrorist attacks last September provided a painfully graphic illustration of the 21st—century threat environment. They unified our nation and mobilized our government in ways that earlier attacks, repeated warnings, and stacks of reports published during the previous decade did not. The difficulty of the challenge ahead—*ensuring the security of our homeland*—is increasingly evident.

In the aftermath of September 11, key instruments of our national power were found wanting. Diplomacy is of limited utility when there is no governing body with whom to negotiate; al—Qaeda attacked *who we are* as a nation rather than *what we do* as a government. Our intelligence apparatus failed to warn of the impending attack—once again highlighting the fault lines between foreign and domestic authorities as well as the vulnerabilities inherent in our open society. Subsequent military action reduced the threat from al—Qaeda but also demonstrated that the military capabilities that conferred 20th—century superpower status are not well matched to our first war of the 21st century—*the global war on terrorism*. The damage inflicted on our nation's

Report Documentation Page

Report Date 00042002	**Report Type** N/A	**Dates Covered (from... to)** -

Title and Subtitle Homeland Security Technologies Creating an Asymmetric Advantage	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Center for Counterproliferation Research National Defense University Washington D C	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor’s Acronym(s)**
	Sponsor/Monitor’s Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes The original document contains color images.	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 12	

economy extended well beyond the lives lost and property destroyed during those horrific attacks and is likely to have long—term ramifications given the shockwaves induced in our insurance industry. But perhaps the most stunning aspect of the September attacks was the subsequent realization that the weapons employed were owned and operated by our own private industry and that the targets were predominantly populated with civilians—breaking all the traditional rules of warfare and shattering the myth that 20th—century national security solutions are adequate for 21st—century threats. On September 11, 2001, the asymmetric advantage belonged to al—Qaeda.

The repercussions of September 11, amplified by the subsequent anthrax—filled letters, breathed new life into old recommendations for increased federal investment in intelligence reform, military transformation, border security, and a diverse suite of emergency response capabilities. In anticipation of budget hikes, government organizations at all levels are being inundated with industry proposals touting technology—based solutions. The interagency Technology Support Working Group received an estimated 12,500 responses to a broad area announcement issued last October inviting proposals for combating terrorism and related topics.[1] Many corporations are not waiting for proposal solicitations but rather are aggressively targeting the nascent homeland security market with their product offerings. Groups such as the National Defense Industrial Association are creating coalitions to keep members informed about emerging issues and opportunities.[2] But the budding homeland security marketplace extends well beyond the federal government, encompassing state and local governments as well as private industry. The shared challenge is to understand the potential—and the limitations—of proposed products, to ensure that expenditures maximize our national return on investment, and to build a synergistic homeland security enterprise that creates an asymmetric advantage for America.

A necessary first step is to more clearly define the desired outcomes—to establish national objectives for the homeland security mission. From those objectives we can devise strategies—the means to accomplish the objectives. From those strategies we can begin to identify opportunities to employ technology—based solutions. And from those opportunities, we can determine where today's products are adequate—given effective implementation—and where today's technologies fall short. Then, and only then, can we create a roadmap to guide technology investment for the homeland security mission. But rather than tasks to be completed in sequence, these steps must become elements of an ongoing process that continually adapts our homeland security posture—maintaining an asymmetric advantage over the adversaries who would threaten our homeland.

Defining National Objectives

The ultimate objective is to *deter* future attacks on our homeland by convincing adversaries that their attack will not succeed or that our nation's response will cripple their cause. Deterrence is most effective when our intent is made clear through policy, when our will to act is evident, and when our ability to act is underpinned by operational capabilities. During the Cold War, our deterrence strategy was based largely on maintaining the *balance of power*; we emerged victorious—the world's sole military superpower. But asymmetric options tilt the balance of power;[3] 21st—century adversaries are likely to have more in common with al—Qaeda than with the former Soviet Union. As suggested in a book published in the aftermath of the September attacks, our strategic mantra for the future should be the *power of balance* rather than the balance of power. That is, deterrence in the 21st century will require an evolving suite of operational capabilities that hedge our bets against thinking adversaries who are equipped with an infinite array of asymmetric weaponry—but investment in such capabilities must be balanced against the societal and economic impact that could accrue from their implementation.

There are two paths to *deterrence*—denial and punishment; operational objectives must support both paths. Focusing first on denial, we can parse an attack into three dimensions—means, motive, and opportunity—and establish objectives for each. One objective is *prevention*—denying an adversary the means to attack, primarily through defensive measures. Another objective is *preemption*—denying an adversary the opportunity to attack, primarily through offensive operations. Finally, our objectives are to effectively manage both the immediate *crisis* and the downstream *consequences* to mitigate the effects—denying an adversary the attainment of the impact that motivated the attack. Post—attack, the dominant driver for punishment is to re—establish deterrence—in the minds of all adversaries, not just those responsible for the given attack. An essential first step is *attribution*—to the immediate perpetrator, but also to the ultimate sponsor of the attack. Finally, our *response* must be both swift and appropriate—as judged by our allies as well as our citizens.

These objectives—*deterrence, prevention, preemption, crisis management, consequence management, attribution,* and *response*—form a strategic cycle of interdependent elements.[4] Success in achieving one objective makes success in others more likely, but failure in one area makes failure in others more likely as well. The essence of an asymmetric offense is exploitation of weakness; thinking adversaries learn from their successes and failures as well as our responses and adapt their approaches accordingly. On the other hand, the essence of an asymmetric defense is exploitation of the strength of the defender. A comprehensive national strategy for homeland security will address each objective in the strategic cycle and will create a comprehensive and synergistic collection of operational capabilities that evolves with sufficient agility to deter—or defeat—thinking adversaries.

Operationalizing the Strategic Cycle

Deterrence

Deterrence must be established in the minds of our adversaries; our success is measurable only through their actions. Deterrence strategy is instantiated in national policy and is supported by operational capabilities that seek to effect denial, punishment, or both. While largely the purview of our national security apparatus, the intelligence analysis required to inform policy development is equally important to the development of homeland security strategies. The most critical shortfall, one that has been repeatedly documented and painfully corroborated, is in understanding our adversaries' objectives—that is, the outcomes they seek to achieve through their actions. Such information is vital if we are to effectively manage the risks inherent in our open society.

From a deterrence perspective, a key strategy is therefore to establish and maintain a robust understanding of our adversaries, a task historically relegated to our intelligence apparatus. From a homeland security perspective, a key strategy must be to share that understanding with those who are developing and implementing operational capabilities to help stop and punish attacks on our homeland. But equally important from a homeland security perspective is to establish a collaborative process that extends well beyond our traditional intelligence apparatus, such that threat assessments are informed by the data and insights gleaned from the homeland security operational environment.

Prevention

Prevention is most effectively accomplished through layers of defenses intended to deny an adversary access to weapons, to delivery systems, or to the target itself. Preventive measures begin with international treaties and control regimes that restrict an adversary's access to specialized materials or weapon delivery systems, but such approaches barely scratch the surface in terms of asymmetric threats to our homeland. This is not to suggest that they are unimportant, only that we cannot rely solely upon such measures—even in areas where control regimes are in place. Acknowledging this reality, our nation's missile defense strategy is motivated by a desire to deny an adversary that delivery option for weapons of mass destruction.

Border security—preventing the entry of illicit goods or personnel—is typically viewed as the first layer of defense for our homeland. Inspection and authentication systems are stressed by the need to efficiently maintain trade and travel while still providing a barrier to external threats. It is increasingly apparent that to balance these competing demands will require international cooperation and coordination; border security cannot begin at our geographic boundaries, nor can it rely upon 100% inspection and individual authentication—although both constitute vital operational capabilities. As noted in a recently published paper describing the importance of maritime domain awareness, "information is the key."[5] An essential improvement to border security is implementation of an integrated system that synthesizes data from disparate sources to enhance tactical situational awareness—as well as to inform evolving threat assessments.

A unique challenge arises in the borderless realm of cyberspace, where there is no way to prevent malicious traffic from entering our nation's networks, but in an era of e?commerce and e—government, robust e—defense is vital. Many serious asymmetric threats stem from sources that cross our borders legally—or virtually—or originate within our borders, thus creating the need for additional layers of defense. Inside our homeland, core preventive measures can be lumped into three broad categories—each with unique challenges, but with the common responsibility to continually enhance national situational awareness as well as our understanding of emerging asymmetric threats. A systemic issue that crosscuts the three categories is the need for a better understanding of interdependencies and shared vulnerabilities—where a risk accepted by one becomes a risk assumed by all.

The first category includes measures to prevent an adversary from acquiring materials, equipment, or knowledge that would enable creation or delivery of an asymmetric weapon. This includes, for example, access controls for radiological materials (for example, medical waste products) and biological pathogens. It also includes the restriction of access to information that could be used to aid terrorist planning activities. The federal government has already taken steps to ensure that data made available via government websites are scrutinized with this in mind, and pending legislation would narrow the rights guaranteed under the Freedom of Information Act in an effort to further protect sensitive information.[6] Such measures contribute to our defense, but implementation is fraught with challenges—relating to policy as well as fidelity, given the dual—use nature of much of the relevant materials and equipment and the inherent difficulty of preventing access to information in a digital world.

A second category of defenses within our homeland includes measures that deny our adversaries the use of our nation's infrastructure as a delivery system for asymmetric weapons—as occurred on September 11 and in the subsequent anthrax letter attacks. Relevant examples also exist in cyberspace, where our information infrastructure has been used to propagate viruses as well as to effect denial—of—service attacks that have caused sizable economic damage. And given the permeability of our border defenses, the potential exists for asymmetric weapons to make their way directly into our internal transportation infrastructure. Many studies have focused on our nation's critical infrastructures as a probable target, but it is equally important to also acknowledge their utility as delivery mechanisms—and to devise measures to prevent such use by our adversaries.

The third broad category comprises perimeter defenses designed to protect high—value targets—that is, to prevent an adversary from delivering a weapon to the target. The first step is to identify likely targets—a process that must be informed by an understanding of our adversaries' objectives. Based on terrorist attacks during the past decade, the target set clearly includes major structures that symbolize America—for example, American embassies, the World Trade Center, and the Pentagon. It takes little imagination, however, to see that corporations that have become global symbols of Americana, special events that attract large gatherings of our citizens, critical infrastructures that underpin our society, and industrial sectors that drive our economy may also be prime targets—depending upon the impact our adversaries seek to achieve. In cyberspace, the perimeter defense metaphor requires the prevention of malicious code from penetrating system boundaries—the challenges are to identify all entry points in an increasingly networked world and to distinguish malicious code from routine business traffic. Comparable challenges exist in other critical infrastructures as well as in our core industrial sectors, but perimeter defenses are needed for key nodes and critical facilities. It is more difficult to envision perimeter defenses for biological attacks, since pathogens may be delivered via life—sustaining substances such as air, food, and water, or propagated by human, plant and animal life. One approach to defending against bio—terrorism is the creation of immune systems that prevent not the attack but the effects;

promising approaches include vaccines, genetic engineering (for example, development of disease—resistant crops), or both, but their ability to counter the diverse spectrum of potential threats is uncertain, and their application is controversial.

Layered defenses are crucial for the homeland security mission—perimeter defenses for the World Trade Center would not have prevented the September 2001 attacks, but preventing the perpetrators from gaining control of the airplanes, by denying them access to the cockpit, would have. On the other hand, perimeter defenses for the World Trade Center might have prevented the 1993 bomb attack. To reap the benefit of our national investment, we must devise a system of mutually reinforcing layered defenses. This is a formidable challenge, given that ownership and operational responsibilities are fragmented and distributed among federal, state, and local governments as well as throughout private industry—and the challenge is compounded by the need for international cooperation and coordination, particularly in areas such as border security and cyber—security.

For the homeland security mission, prevention is the most complex of the seven objectives that make up the strategic cycle, although all objectives pose significant challenges. Our open society is infinitely vulnerable to asymmetric attack; the advantage is currently on the side of an adversary. The goal must be to continually raise the bar through defensive measures that make our adversaries' task more difficult—and to ensure that we learn from their attempts just as they do. But the dilemma is to decide how much defense is enough—that is, to effectively exploit the *power of balance*. An optimal system will integrate a nationwide array of preventive measures the sensitivities of which are adjusted—in near—real time—according to the level of threat, and the synthesized sensory data of which enhance tactical situational awareness while informing an evolving assessment of asymmetric threats to our homeland.

Preemption

Preemption is typically an offensive operation motivated by our desire to deny an adversary the opportunity to attack our homeland. Enduring Freedom is a preemptive military operation that seeks to deter future attacks by al—Qaeda. Similarly, the detainment of visa violators in the aftermath of the September attacks may be viewed as a preemptive action by our law enforcement apparatus. Such operations, while essential to homeland security, are fraught with risk. Preemption on foreign soil must be justified by compelling intelligence that persuades allies that our actions are warranted—we will be judged by world opinion. Preemptive operations on American soil must be equally well justified lest they threaten our constitutional freedoms in the eyes of our citizenry. But knowing why preemption is warranted is just the beginning; the next step is to know when and where a preemptive operation is possible—with a level of precision that is difficult to achieve. So once again, solid intelligence—rapidly shared with those in a position to act—is a critical operational capability.

Crisis Management

Crisis management is the investigation and law enforcement response to impending or actual attacks on our homeland; a key issue is rapid assessment of the situation to inform decision making. Historically, we have treated attacks as local events, but the attacks on September 11 highlighted the need for more expansive situational awareness. The fact that passengers on the fourth hijacked airplane learned of the earlier attacks on the World Trade Center motivated actions that, in all likelihood, prevented an even more devastating outcome—denying al—Qaeda their intended objective for that airplane. Crisis management capabilities to support the homeland security mission must facilitate coordinated response to geographically separated but simultaneously orchestrated attacks—as well as to sustained campaigns of attacks.

Unique challenges are posed by biological and cyber—threats since there may be no discernible ground zero, and the onset of effects may be significantly delayed relative to the time of attack. Medical technicians, veterinarians, or computer systems administrators may be the first to detect symptoms, and in the early stages, in the absence of a broader view of the situation, it may be difficult to determine that an attack has occurred. In addition, some biological and cyber—weapons possess viral characteristics that amplify the impact of the original attack—further limiting our ability to predict how the crisis will unfold. In such cases, we are likely to be managing the consequences before detecting a crisis.

Asymmetric threats impose new demands on crisis management systems. From a homeland security perspective, we need far better mechanisms to rapidly assess and monitor the situation from a national—and perhaps even international—perspective. In addition, secure communications that link on—scene authorities to national crisis response centers are essential, as is an information dissemination mechanism that helps decision makers share information with the public to stem the panic that might otherwise exacerbate the crisis.

Consequence Management

The primary goal of consequence management is to limit the effect of an attack—thus denying an adversary the achievement of the desired impact. Many reports describe first?responder requirements for protective gear, interoperable communications, and training, as well as exercises to bolster their experience with low—probability, high—consequence attack scenarios. But given the vast array of asymmetric options, also needed is real—time identification of residual materials that may pose unseen threats to first responders as well as to the surrounding public. Such capabilities are important not only during the early stages when the focus is on rescue of personnel, but also during later stages when reconstitution of functionality may require physical decontamination. And, as evidenced by the aftermath of the anthrax attacks last fall, our capability to decontaminate facilities needs considerable improvement.

Once again, unique challenges are posed by the biological and cyber—threats, since effects may be widespread before an attack is detected—significantly impeding our efforts to limit the impact. And once again, national situational awareness is a critical enabler, as is the capacity to rapidly mobilize the requisite consequence management capabilities at geographically disparate locations. A medical surveillance system designed to rapidly detect anomalous outbreaks of disease would help manage the consequences of a biological attack against humans, but the equivalent is needed for plant and animal life. Similarly, our information infrastructure must be equipped with intrusion detectors that feed their data into a system that synthesizes the information to create real—time situational awareness, and that knowledge must be continuously accessible by those who are positioned to take action to limit the impact of an attack.

Mitigation of the psychological impact of an attack is another important aspect of consequence management—particularly given that our adversary's objective may be to instill fear throughout our nation, or even to shake the confidence of the American public in its government's ability to defend our homeland. The immediate reaction to the September 11 attacks was shock and horror, but the subsequent threat warnings induced an unprecedented level of anxiety in many Americans—our economy continues to suffer due to the ongoing reduction in tourist air travel. Similarly, our early inability to assess and communicate the situation with regard to the anthrax mailings amplified the deleterious effects well beyond the lives lost and property contaminated by the letters. Thus, a trusted and reliable information dissemination system is an essential operational capability. But to be fully effective, such capabilities must be used continually to educate the public with regard to potential threats as well as to warn of impending attack and recommend individual actions—so that when an attack occurs, the public has a trusted source of information to help mitigate the psychological impact, during the crisis as well as in the aftermath.

Attribution

Attribution is the linchpin of the strategic cycle; without attribution there can be no response; without attribution there will be no deterrence. Traditional warfare leaves little doubt regarding the identity of the adversary—missiles typically come with return addresses—but the same cannot be said for asymmetric attacks on our homeland. This is perhaps best exemplified by our inability to rapidly identify the individual(s) who mailed the anthrax letters. Our law enforcement apparatus takes the lead in gathering on—scene forensic data as well as in the subsequent investigation, but it is painfully clear that timely attribution of asymmetric attacks requires new investigative capabilities.

Attribution is particularly problematic for attacks that have no ground zero—as well as attacks with delayed effects. Biological attacks—whether the target is human, plant, or animal—are especially difficult, since early symptoms may masquerade as naturally occurring disease. Cyber—terrorism poses comparable challenges due to the anonymity of cyber—space, coupled with an adversary's ability to launch a virtual weapon without setting foot on American soil. A nationwide system that synthesizes data gleaned from the various defensive mechanisms could speed the attribution process by narrowing the scope of the investigation, but also needed are forensic capabilities that are better matched to emerging asymmetric threats.

Response

Our nation's response to any attack on our homeland is likely to be multipronged; it may include preemptive military, law enforcement operations, or both, as well as criminal prosecutions. Post—attack, the immediate desire is to punish the adversary for the actions, but our end goal is to deter future attacks. We routinely employ the so—called paradox of power [7] —the use of violence to protect against violence—as a means of punishment; our dilemma is to know whether such actions cripple the cause of our adversary or in effect strengthen the adversary's cause by creating martyrs. So once again, our actions must be guided by a solid understanding of the motivations of our adversary—calibrated by the adversary's value system rather than our own.

Given the strength of our military, it is unlikely that an adversary will declare war—in the traditional sense—prior to an attack on our homeland. Our response must therefore maintain a tenuous balance—appropriately punishing the causal attack as well as seeking to deter future attacks, but without alienating our global allies.

Setting Investment Priorities

The challenge—*ensuring the security of our homeland*—is immense; the preceding discussion only hints at the complexity of the task ahead. The events of September 11 reenergized the debate about who is in charge of this formidable task. Executive Order 13288, signed on October 8, 2001, created the Office of Homeland Security, the mission of which is “to develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks.”[8] The Office of Homeland Security wields the clout of the President but possesses no statutory authority, and the executive order did little to clarify operational responsibilities within the federal government. But given that mission responsibilities are shared with state and local governments as well as with private industry, even perfect clarity regarding mission boundaries inside the federal government would do little to reduce the complexity of the task confronting us.

Initiatives and priorities for homeland security were established by the President to guide budget development for FY03 [9], but legacy mission responsibilities will inevitably bias organizational funding requests. Although not an argument for restructuring the federal government, the current situation is unlikely to maximize the national return on investment from a homeland security mission perspective. Definition of the national strategy—due early this summer—will help, but it must be accompanied by clear objectives and measurable outcomes for which individual organizations can be held accountable. Since the Office of Homeland Security has no statutory control, it must influence investment and exploit the results to accomplish its assigned mission.

Asymmetric attacks are typically characterized as low—probability, high—consequence events. Even if there is significant general threat of attack, the probability that any specific location will be attacked is likely to be low; but if it is attacked, the consequences could be disastrous. This led the President to place initial budgetary priority on items that have collateral benefit and to declare that our national strategy for homeland security will “seek opportunity out of adversity” [10] through preferential investment in capabilities that improve our daily lives while enhancing the security of our homeland. This is, and should remain, a guiding principle for homeland security resource allocation.

To maximize our national return on investment, we should invest first in areas that support multiple objectives within the strategic cycle and are broadly applicable across the diverse spectrum of asymmetric threats. But given that we are unlikely to successfully deter, prevent, or preempt every attack, we also must invest in capabilities to help mitigate the effects of a potentially catastrophic attack.

Strategic Intelligence—for Unconventional Threats

Better understanding of our adversaries—their values, their motivations, and their capabilities—is fundamental. Such knowledge must guide our homeland security investment in preventive measures, in consequence management capabilities, and in tools to aid attribution. This is not a new requirement, but it requires new thinking and new approaches. While primarily the responsibility of our intelligence apparatus, owners of the homeland security mission must implement a process to define their needs, establish performance objectives, and monitor results—and they must willingly contribute their insights regarding the operational threat environment.

Information Sharing—to Enable Distributed Decision Making

The need for timely sharing of information with those who must take action is well documented—but unfulfilled. Information regarding the threat underpins strategies and enables tactics for each of the seven objectives. The operational community for homeland security—decision makers who need information—includes 40—plus agencies within the federal government that have responsibility for various parts of the mission; it includes state and local government authorities that will be on the front lines of crisis and consequence management in case of an attack; it includes private corporations who own and operate much of our nation's infrastructure—and may be directly targeted for attack; and it includes the citizens of our nation who will be impacted—whether physically, financially, or emotionally—by an attack on our homeland. While the requirement for sharing of information is pervasive, the need—to—know paradigm still has merit—not everyone in the homeland security community needs access to all information. But we must explicitly acknowledge and effectively support the broad community of decision makers by providing them with timely access to the information they do need—within their operational context. That is, we must share information that enables them to make operational decisions rather than merely provide access to data.

Synergistic Enterprise—to Create National Situational Awareness

The asymmetric threat cannot be countered with stovepiped solutions, nor can we assign total operational responsibility to any single entity. Today, the whole is less than the sum of its parts—we do not know as a nation what is known to an individual organization. But we cannot afford an array of solutions that is equal to the sum of its parts—the vulnerabilities are too great and asymmetric options too diverse. Instead, we must build a synergistic enterprise—a whole that is greater than the sum of its parts. We must create a *central nervous system* for the homeland security mission; it will enable us to more rapidly detect an attack, to more effectively manage the consequences, and to more rapidly achieve attribution—it will also enable us to more efficiently cope with the vandalism, crime, and health care issues that plague our society. Insights gleaned will advise our ongoing investment in preventive measures as well as in other vital operational capabilities. Such an enterprise will enable us to hedge our bets against uncertainty; it will provide the agility needed to counter thinking adversaries and emerging threats; it will create an asymmetric advantage for America.

Mitigation—to Avoid Catastrophe

Some asymmetric options pose threats so horrific that we must prepare now to mitigate the impact of an attack should it occur. The President has already identified bio—terrorism as a high—priority issue, [11] but a national strategy is desperately needed. This threat poses unique challenges in practically every phase of the strategic cycle. We must deal with the important issues of deterrence, prevention, and attribution as well, but the first order of business must be to establish disease surveillance mechanisms—for plants and animals as well as for humans—to enable rapid detection. Also important are robust treatment options to enable containment and minimize effects, plus communications strategies to mitigate the panic engendered by such an attack.

Investing in Solutions vs. Buying Technologies

Just as technology provided the foundation for national security strategies in the 20th century, technology will enable 21st—century strategies for homeland security. But technology—based *solutions* will comprise a holistic approach that includes *technologies* enabling *processes* implemented by well—trained *people* operating in concert with established *policies*. In the national security equation, advanced technology may yield superior weaponry, but our military superpower status is based on warfighting capabilities underpinned by doctrine that is constrained by policy and supported by training to enhance operational execution. The same holistic approach is required for the homeland security mission.

As homeland security strategies are established, we must be particularly cognizant of the potential insider threat. Ownership and responsibilities for various aspects of homeland security are distributed throughout federal, state, and local governments as well as private industry. This means that policies and processes must deny adversaries the opportunity to become insiders to our homeland security solutions.

A vast array of technologies is needed to accomplish the homeland security mission. Some technologies will yield near—term solutions—if effectively implemented. Some technologies have matured for different purposes and therefore require adaptation or integration to support the homeland security mission. And, inevitably, some technologies that will be important to securing our homeland have yet to be discovered. A technology roadmap for homeland security must address all three categories, but each will require a different approach.

Implementation

After definition of the needed operational capabilities, acquisition of commercially available products or services—given that they meet mission needs—is the preferred approach. But such acquisitions must not occur without clear definition of guiding policy, operational process, and personnel training requirements to achieve effective implementation. These are simply the basics of good business. But from a homeland security perspective, the fragmented operational environment complicates the task—particularly given the need for our homeland security solutions to work as a synergistic enterprise. We must avoid implementation of local solutions that create new fault lines; while a single approach is not feasible, definition of national standards and identification of best practices—including policy, process, and training—will better leverage our nation's investment.

Innovation

Significant opportunities exist to adapt or integrate technologies already in use elsewhere to provide solutions for the homeland security mission. Such application may require changes to policy or operational process in addition to some technology development. Many examples exist, such as fraud—detection techniques in use in the financial services industry but potentially applicable to analysis of our adversaries' financial transactions, and multimodal biometrics systems that may be useful for access control applications. What is needed is an environment that fosters experimentation and adaptation of such capabilities in conjunction with the necessary policy and operational processes to yield a homeland security enterprise solution.

Invention

Some asymmetric threats simply cannot be effectively countered given today's technologies; a sustained research program is needed to discover or invent the requisite tools. But such problems are rarely unique to the homeland security mission, so a significant opportunity exists to leverage investments made elsewhere—by government as well as by industry—through cooperative research portfolio management. The challenge will be to ensure that research results are adapted to the homeland security mission and implemented as an enterprise solution.

Sustaining the Asymmetric Advantage: A Manhattan Project for the 21st Century

This nation's greatest technological endeavors have been inspired by fear and motivated by competition—a desire to get there first. In the late 1930s, fear that Hitler's Germany would build the world's first atomic bomb stimulated the Manhattan Project—a top—secret engineering venture that engaged the best available scientific expertise and delivered a working atomic bomb—the device that was used to bring an end to World War II and served as the foundation for our deterrence strategy throughout the Cold War era. The Soviet Union's launch of Sputnik in 1957 led to the creation of the Advanced Research Projects Agency (ARPA) and subsequently inspired the race to space, which was motivated by our desire to “be in a position second to none.” [12] ARPA developed our nation's first successful satellite [13] and later turned its attention to computer networking with the goal of creating a communications network that was immune to a nuclear attack; the result was ARPANET, precursor to today's Internet. [14] Technological advances spawned by these efforts have shaped our society and fueled our economy.

The term *Manhattan Project* is now “a byword for an enormous breakneck effort involving vast resources and the best scientific minds in the world.” [15] The original Manhattan Project addressed a grave threat to the security of our nation. Today we confront a grave threat to the security of our homeland, and it is again one that cannot be countered with the available national security solutions. Now, as then, we need a breakneck effort—to overcome institutional inertia as well as to address the immediacy of the threat. Now, as then, significant resources—both dollars and scientific expertise—will be required. But the similarity stops there. The homeland security mission will not be served by a massive government project conducted in secrecy. Countering the asymmetric threat requires defense as well as offense, and American citizens are on the front lines of the battle.

The original Manhattan Project was initiated to invent the necessary technologies and to implement those technologies in a solution that would be employed by our nation's military; it was a finite project with a clearly defined goal. But there is no silver bullet that will define success for the homeland security mission—the dynamic landscape of asymmetric options demands an evolving suite of operational capabilities—capabilities that will be employed not only by a variety of agencies within the federal government, but by state and local governments and private industry as well. And a vast array of technologies that will yield near— and mid—term solutions exists today—not only in government laboratories, but also throughout the commercial sector. While some invention is needed, the immediacy of the threat will not allow us to defer initiation until the research is completed, and the changing nature of the threat will require an ongoing research effort.

What is needed today is a *homeland security laboratory enterprise* that supports implementation, innovation, and invention of solutions for the *homeland security operational enterprise*. The purpose is not to replicate what is more effectively accomplished by commercial industry or academia, but rather to complement and facilitate their efforts—to maximize our national return on investment.

It is instructive to note that while the Manhattan Project was finite in duration, what is now the Department of Energy's national laboratory system maintains ongoing stewardship responsibility for the nuclear weapons program that the Manhattan Project began. Today we must initiate an effort comparable to the Manhattan Project—that is, we must mobilize our nation's best scientific expertise to help ensure the security of our homeland—to create an asymmetric advantage. But we must, from the beginning, build the national infrastructure needed to support the homeland security operational enterprise for the long haul—to sustain the asymmetric advantage.

Facilitating Implementation

A homeland security laboratory enterprise would *facilitate implementation* by fostering the definition of national standards to ensure interoperability across the operational enterprise by identifying and disseminating best practices to enable more effective local implementation and by establishing performance benchmarks to inform the vast community of buyers of homeland security solutions. In addition, it would maintain test facilities to support specialized product evaluation (for example, personal protective equipment, sensors, and decontamination techniques) and demonstration facilities to support operational exercises for low—probability, high—consequence scenarios.

Enabling Innovation

A homeland security laboratory enterprise would *enable innovation* by providing an environment to bring together potential solution providers and end users for the purpose of experimentation and mutual education—that is, to enhance the solution providers' understanding of operational constraints, as well as to increase end users' awareness of the art of the possible. Such an environment would serve as a bridge to speed insertion of new technology—based solutions into the operational enterprise. The laboratory enterprise would establish tentacles into the operational enterprise to ensure a robust understanding of the needs, into industry to identify technologies with potential applicability, and into research communities—in academia, industry, and government—to identify breakthroughs that show promise. And it would maintain working laboratories to support collaboration, experimentation, and adaptation to create solutions for the operational enterprise.

Fostering Invention

A homeland security laboratory enterprise would *foster invention* through cooperative research portfolio management—leveraging relevant investments by others regardless of the funding source. The portfolio's investment objectives would be to accelerate progress, to fuel competition, and to ensure that the full spectrum of needs is addressed.

Creation of a homeland security laboratory enterprise with the requisite characteristics will not be easy. If the mission is assigned to an existing organizational entity, explicit strategies will be required to overcome the legacy baggage and institutional inertia that would otherwise ensure its demise and to establish the trust and the collaboration that will be essential for its success. But creation of a completely new entity to execute this mission would be too costly and too slow. What is needed is a hybrid approach—a new core organization to provide enterprise management for a networked laboratory system that comprises relevant capabilities residing within today's government laboratories, together with a limited set of facilities chartered to support unique mission requirements.

The homeland security laboratory enterprise management organization would ensure that the necessary facilities were available—but it would not own those facilities. It would ensure that results—successes as well as failures—yield lessons that are learned throughout the operational enterprise as well as the laboratory enterprise. It would resolve the policy issues that might otherwise impede insertion of new technologies into the operational enterprise. It would motivate technology transfer via equitable management of intellectual property rights. It would maintain a technology roadmap for the homeland security mission to guide the research portfolio. And it would establish performance measures and incentives for its partners—in industry and academia as well as the government. The objective of the homeland security laboratory enterprise is to exploit our nation's technological innovation to sustain the asymmetric advantage over our adversaries. Its success would be measured by its impact—solutions deployed in the homeland security operational enterprise.

In Conclusion

The homeland security mission cannot be described by projects to be completed or systems to be acquired—although those will be important components of strategy implementation. Ensuring the security of our homeland means protecting life—and our way of life—against those who wish to eliminate it. It means marshaling the strengths of our nation—our technological prowess and our capacity for innovation—to defeat those who seek to destroy our nation.

The challenge—*ensuring the security of our homeland*—demands bold action and sustained focus. The federal government must provide the leadership, but mission responsibilities are shared with state and local governments as well as with private industry. It is trite to describe once more the need to eliminate the stovepipes that exist in the current environment, but we can no longer afford the fault lines created by political boundaries and organizational turf. To defeat a networked adversary will require a networked nation. To counter technology—enabled threats will require a technology— enabled response. And to prevail in the face of uncertainty will require a synergistic enterprise.

---

[1] "Tech Support Group Finishing Review of New Combating Terror Ideas," *Inside the Pentagon*, March 14, 2002.

[2] "Defense Contractors Shuffling to Win Homeland Security Markets," *Inside the Pentagon*, January 31, 2002.

[3] Kurt M. Campbell and Michèle A. Flournoy (principal authors), *To Prevail-An American Strategy for the Campaign Against Terrorism* (Washington, DC: CSIS Press, 2001), ISBN 0-89206-407-2, p. 22.

[4] "Homeland Security: The Strategic Cycle," http://www.homelandsecurity.org/Hls/StrategicCycle%2Edoc.

[5] James M. Loy and Robert G. Ross, "Global Trade: America's Achilles' Heel," *Defense Horizons*, February 2002; http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=33.

[6] "Risks Prompt U.S. to Limit Access to Data," *Washington Post*, February 24, 2002.

[7] James Dale Davidson and Lord William Rees-Mogg, *The Sovereign Individual* (New York: Simon & Schuster, 1997), p. 174.

[8] Executive Order 13288 Establishing the Office of Homeland Security and Homeland Security Council, October 8, 2001.

[9] "Securing the Homeland, Strengthening the Nation," President George W. Bush; http://www.whitehouse.gov/homeland/homeland_security_book.html.

[10] Ibid.

[11] Ibid.

[12] President John F. Kennedy, 1962; cited in the National Air and Space Museum online exhibit "Space Race"; http://www.nasm.si.edu/galleries/gal114/.

[13] NetValley, "1957: Sputnik Has Launched ARPA," in "History of the Internet and WWW"; http://www.netvalley.com/intval-zagotovka3-0327-25.htm.

[14] Yahoo! "Birth of the Internet"; http://smithsonian.yahoo.com/internethistory.html.

[15] U.S. Department of Energy, Office of Environmental Management, "The Manhattan Project"; http://www.em.doe.gov/circle/manhattn.html.